Organized Crime and Cybercrime
Criminal Investigations and Intelligence on the Cutting Edge

Technical Report –
Information Technology Series

by

Marcel-Eugène LeBeuf, Ph.D.
Mlebeuf@rcmp-grc.gc.ca

Police Sciences School
Canadian Police College

Ottawa, 2001

Ce document est aussi disponible en français :
www.cpc.gc.ca

Table of Contents

Summary i

Acknowledgments x

General Introduction 1

1- Current Technological Developments and Their Impact on the Police 2

2- Investigative/Criminal Analysis, Practices, and Procedures 8
2.1- Crime Investigation Practices 10
2.2- Investigation Methods 14
2.2.1- Crime Response Joint Force Operations 19

3- Intelligence and Its Uses 22
3.1- Purposes of Gathering Police Information 23
3.2- Quality and Use of Information 25
3.3- Information Sharing – Myth or Reality? 27
3.3.1 Non-Sharing Factors 29
3.3.2 Conditions for Sharing Information 33
3.4- Databank Supply Problems 36

4- The Need for Adequate Training 39
4.1- Development of Critical Success Conditions 43

Conclusion 46

References 49

105-02796/

Summary

Introduction

This report deals with two major issues: criminal intelligence and investigation practices in an environment shaped by the emergence of information technology and the recognition that police information must be shared. We assess, based on available technological tools for criminal intelligence units, including databanks, investigators' concerns about data collection, data entry, and retrieval. We also look at the emphasis placed on data sharing. In addition, we try to determine to what extent the traditional isolation between units, as it relates to investigation practices, contributes to a successful investigation and, more generally, to the successful sharing of data collected for that purpose.

We met with investigators, investigation unit managers, and deputy police chiefs from several police departments throughout Canada. We selected members of joint force operations (JFOs), where several police departments co-operate on an investigation, for instance on outlaw motorcycle gangs, and also more traditional investigation units such as drugs, homicides, economic crime, etc.

Information technology is rapidly evolving and spreading across organizations, governments, and society. Technology is particularly conducive to innovation, and it gives rise to a new work culture.

In Canada, a two-pronged initiative by the federal government warrants special attention. The first prong, called Government On-Line, is aimed at increasing electronic transactions between the government and the community and developing the legislative tools required for large-scale electronic commerce. The second prong focuses on reinforcing user confidence, improving the electronic commerce information infrastructure, and optimizing its benefits.

The criminal environment is also changing. The Internet has boundless growth potential, but its potential for legal use is matched by an equivalent potential for illegal use.

Given that fighting organized crime is one of the priorities of the federal and provincial governments, two major issues intersect:

- generating intelligence and information to develop effective strategies
- understanding and recognizing the technological tools used by the community, the criminal world, and the police.

The question is therefore how to conduct an investigation when information technology is involved in the crime? This question is especially relevant in terms of the investigation practices used in the field given

the significant changes occurring to organized crime in Canada.

Investigative/Criminal Analysis, Practices, and Procedures

In the field of investigations, as elsewhere, work habits and learned approaches die hard. After basic training, continuous development, and on-the-job training, "giving up old habits" is not easy. In a changing and evolving environment, police officers and investigators use the technological tools at their disposal non-systematically.

Criminal Investigation Practices

For investigation and analysis purposes, information technology is still perceived as new and threatening.

This perception has many consequences at various levels. The first major consequence is that the police environment should have been prepared to deal with these technological advances before police officers, investigators, and analysts were asked how they used the available technology. A second consequence is directly related to the recommended and actual uses of technology. With technology readily available, the use of computers and computerized databanks tends to become systematic depending on the unit involved.

Personnel and skill development aimed at specific groups, including investigators, is now part of the evolution of the police. Skill development is all the more critical since police officers are not ready to investigate technological crimes because they are unfamiliar with such technology as the Internet or are unable to measure its impact.

Developing advanced technology skills leads in turn to major problems for the police. The promotion process is such that even highly trained individuals must leave their field of expertise to get a promotion. These individuals lose some of their know-how while away from their specialty.

One unexpected consequence of technology has to do with workload. Collecting information and loading it into databanks is viewed as extra work.

It would be incorrect to say that the use of technology is related to age or seniority. It has to do above all with the development of the right attitudes. Furthermore, it is only normal that individual learning, program training, and assistance to co-workers would go through an adjustment period. Finally, increasingly sophisticated specialized services help police officers carry out tasks such as capturing data from hard disks.

Investigation practices are affected by an easy access to technological tools such as computers and by the underused potential of devices such as CD-ROMs. We need both to arouse the curiosity of individuals and to develop their skills.

Investigation Methods

We looked at the traditional separation of investigation tasks as reflected in the creation of various units. These separate units, i.e., economic crime, homicide unit, drugs, etc., impede contacts between police officers either for traditional or cultural reasons.

There is a real and necessary separation between investigation units. This isolation is due to the development of cutting-edge expertise to meet investigation challenges specific to each unit.

This produces obvious turf battles between units—some with a major public impact. Separation also encourages the development of cutting-edge expertise in some areas.

Crime analysts are one category of investigation experts. Investigators need analysts. Their job mainly involves managing complex information, providing direction for specific investigations, and making sense of various elements connected to the investigation.

A formal hierarchy exists among investigation units. This hierarchy has consequences in terms of publicity, major budget allocations, and availability of technological tools such as cell phones, computers, pagers, etc. for individual unit members.

Joint Force Operations

Joint force operations (JFOs) include officers from various police departments and, if required, departmental law enforcement officers. The aim is to combine different forces, for example, to fight organized crime.

Joint force operations are not new, and they are expanding as a concept. Combining efforts leads to better co-ordination of response options, investigative approaches, and budgets. JFOs are now considered the preferred solution for twenty-first century policing, thanks to ad hoc alliances. Also, they provide response options to units and sections that have neither the time nor the equipment to act on their own.

The success of joint force operations is impeded by at least two problems. The first has to do with the fact that individual skills and expertise are not at the same level. The second pertains to personnel management within units, as individuals on loan do not report to the team manager for their annual

assessment, leave, etc. On the other hand, a major positive factor is that information sharing is made easier.

Intelligence and Its Uses

The information contained in computerized databanks and police files is used as a work tool for specific investigations. It helps identify the best targets for effective police actions.

Purpose of Gathering Police Information

These reasons were divided into three categories. First, this information provides direction to the investigation or to the officers. Second, this information is used to improve the quality of operations and to conduct thorough analyses. Third, this information is used specifically to prepare affidavits. It is assumed that the information is up to date and of a high quality.

Quality and Use of Information

Investigators must have access to this information and be capable of interpreting it properly.

A basic concern with respect to information is making sure the most comprehensive collection possible is done. What matters is not so much collecting information as collecting quality information. Quality information leads to arrests and convictions. A lack of co-ordination between the various systems and, incidentally, between police departments contributes mightily to the poor quality of the collected information. Finally, it appears this information is sometimes used for secondary purposes, such as bragging rights for the police department, and then it is shared with others.

Information Sharing – Myth or Reality

Information sharing is in itself a basic problem for the police. It involves co-operation between officers within a department and also between police departments nationally and internationally.

All contacted individuals agreed right away, each in his or her own way, that information sharing is important in principle. Sharing is subjected to a series of formal and informal factors to protect the information, the investigators, the information sources, and the investigation itself. Depending on the situation and the type of investigation, the information is sometimes not shared within an investigation team. Naturally, in such instances, the information would not be provided to other members of the police department or to other departments in Canada or abroad. The time needed and the various systems are impediments to individuals.

Non-Sharing Factors

At least four sets of factors were identified.

The first is the mutual trust created and built between individuals and organizations and supported at all levels within the organizations. Without trust, people are generally reluctant to share anything. The second set covers the legal aspects. The third-party rule applies, i.e., the information and sources may not be disclosed if the third party refuses to do so. Also, privacy protection and access to information legislation is used to control, or rather circumscribe, the information sharing and protection rules. Finally, sharing information with international organizations is also an issue. The third set has to do with investigation methods, including personal attitudes, methods learned on the job with colleagues, and unfamiliarity with computer systems. The fourth set includes working conditions such as physical limitations for recording information.

Depending on their security clearances, department members have access to databanks. Storage systems and technological storage tools do not always facilitate information sharing. The time needed and the various systems are impediments to individuals.

Conditions for Information Sharing

Various information-sharing conditions are related either to personal philosophy or structural obligations. In terms of personal philosophy, failing to disclose information to other members of the unit within a joint force operation would be inconceivable. Supplying information is encouraged. Another condition involves the time of disclosure of the evidence. Here, the information on file could no longer be kept under wraps as the court and lawyers would already be aware of it. The last condition facilitating information sharing is said to be related to a lack of resources to conduct investigations effectively.

Information and intelligence have a different impact depending on the type of investigation being conducted. However, the traditional isolation of investigation units is an obvious drawback in this regard. Police methods will ensure that any responses are suited to the definition of the crime. The collection, storage, and sharing of information are still totally restricted to the unit involved. Within units, sharing information between members of different departments causes friction. Outside the units, a wall of silence and an unwillingness to share information occurs.

The conditions fostering little or no encouragement to share information are two sides of the same problem. Both provide elements of understanding and solutions. Still, information sharing is being practiced today, if only through the large databanks such as the Canadian Police Information Centre. This certainly is a major undertaking for law enforcement. However, for highly specialized and less-specialized investigations, information provides not only direction, but a starting point for investigators.

Problems with Supplying Databanks

Information sharing necessarily implies that the information was previously collected. This also means that the data are valuable for the investigation or investigator or for response strategies.

One of the principles of a good databank supply process is that when a piece of information is not used in an investigation file, it is recorded in the databank to be used by someone else. Current investigative practices make investigators focus on very specific information for their investigation while the so-called secondary information is discarded.

At least four factors affect databank supply practices. The first has to do with how to proceed or the learning of work methodologies. The workload carried by investigators becomes an argument for the partial or non-supply of databanks. The second factor deals with information sources. What information should be collected. Most of the investigators interviewed seemed to agree that the information collected should be current and up to date so that it can be of direct use in the course of the investigation. The actual collection and the efforts required to make sure the information is relevant are seen as demanding and burdensome. Several investigators feel information has a direct bearing on the investigation and can even be used as evidence in the courtroom or lead to arrests and convictions. The third factor involves information sources and benefitting the most from potential sources. The fourth factor is technology. The unavailability of technological tools appears to be a problem. Also, there is a shortage of human resources to enter the data into the banks.

The Need for Adequate Training

The need for adequate training was clearly recognized by the people interviewed and by many others involved in law enforcement. Some feel this training must be specialized so that police officers can remain current in their areas of expertise. Training must be provided in a timely fashion, which does not seem to be the case for a large majority of those interviewed. Finally, one of the main problems with investigator training is personnel rotation.

Learning is sometimes done in the field over time.

Some of the people interviewed were in a position to assess the consequences of a lack of adequate training or of partial training done on the job with colleagues. Those who receive little or no training must inevitably rely on co-workers to get information and advice. This leads to a significant waste of time for both the newcomer and the experienced officer. The need to constantly rely on others, at least for a time, can potentially lead to mistakes or make people reluctant to act. Even more dramatic consequences can ensue, including the loss of expensive cases because of legal errors.

Individuals were asked if specific topics and issues should be included in training programs. Developing training programs and placing a greater emphasis on specialized and issue-oriented training to meet specific needs appear to be important.

In addition, training covers above all the development of legislation and case law. Both have an impact on work practices and methods.

Investigator training, especially in organized crime and cybercrime, was not systematically provided to interviewed officers no matter which police department they worked for. Training programs dealing with investigation levels—beginner or advanced—were seen as relevant by those who took them, i.e., very few of those interviewed. On the other hand, there was a consensus on the need for investigators to keep up to date with regard to evolving legislation, case law, and skill development.

Some of the people interviewed pointed out that specific budgets are too often affected by cuts. Over the long term, this definitely affects police practices by producing blunders, legal errors, or simply improper investigative methods.

Development of Critical Success Conditions

Conditions for an investigation to run smoothly include a large enough staff, an adequate budget, relevant training, use of cutting-edge technology, etc. Training programs have no impact on most of these factors. However, they may potentially affect attitudes and feelings. They can also enhance individual skills.

The real challenge for investigators, and we should also include analysts here, is to sort out the facts using their judgment, intuition, and deductive powers. These aspects are all the more important because information technology has created new means of communication, a new language, new ways of doing business, and new cultural phenomena called hacking, cracking, and phreaking. Police officer training programs probably do not emphasize enough the qualities to be developed because to do so would require a major personnel investment over the short and long term and would involve a certain departure from the classroom-as-a-magic-solution principle. These qualities seem to be directly linked to the information technology culture. This culture requires not only understanding the language of computers, but also becoming familiar with the new computer environment.

In a fast-changing world, future investigators will need to have the following qualities: experience, proficiency, good analytical abilities, and enough flexibility to adapt their work environment to technological advances, future legislation, and the enforcement of this legislation. Another benefit would be the creation of a network system with the help of high-tech companies.

The training should include not only policing techniques but also exercises on logic, deduction, and

assessment of difficult cases. Scenario-type exercises should encourage student input while testing students' understanding, development capacity, and their deductive abilities.

Other potential solutions should be explored. They include partnerships between the police and various groups involved in security. They also involve alliances with government agencies and other countries. But how can they be kept up to date? Each organization has to follow legal standards, work practices and ethical rules. What is at stake for each? What is the information sharing capability of each? What tools are available to do this? What limitations are placed on sharing personal information by privacy legislation? What are the technical hurdles? These are major points that need to be addressed to be able to achieve partnerships to fight crime.

Presumably, tools, work methods, and common interests could be shared through seminars providing advanced training consistent with the reality of the organizations involved.

Partnerships can also be demonstrated through specific co-ordination among law enforcement agencies. One can envision the creation of a databank that would be used, for example, for sophisticated technological crime or for action models, in order to be able to develop prevention programs. One can also see drawing a list of law enforcement players or units dedicated to organized crime and cybercrime. Surveys conducted by specialized firms on the penetration of computer systems could be very helpful to the police in their decision-making process.

Conclusion

Existing limitations affecting investigations can be summarized as follows: There is a staff shortage, and the personnel is constantly being rotated. For instance, investigators from the homicide unit are sometimes seconded to other units. The computer crime sections may also be too small. In addition, individuals frequently have to leave an investigation unit to be eligible for a promotion. These investigators take their expertise with them and then have to develop another.

Furthermore, budgets are too often inadequate or insufficient to provide the tools required to conduct effective investigations.

Investigator training is not always suited to the context, is not always timely, or is not received at all. It is, however, considered essential.

For information technology-related crimes, there is a requirement to develop investigative skills aimed at understanding what to do rather than trying to become an expert in data processing or systems management. There is a large pool of experts in the field of technology; police officers simply have to learn to work with them.

Concerning cybercrime, computer terrorism, and the new types of environmental crimes, there is an obvious lack of knowledge about problems and issues. More often than not, the people interviewed thought these came under the responsibility of specialized units or agencies other than the police. This suggests that law enforcement does a poor job of preparing the officers to deal with an evolving society.

Finally, a few more comments. There definitely is an investigation culture. In this culture, individuals are kept in separate boxes, sometimes referred to as silos, which is an impediment to mutual co-operation, to information sharing, and ultimately to a successful investigation. A potential solution would be to use joint training programs through which co-operation, sharing, and the ability to get expertise wherever it can be found would be taught and encouraged. Today, sharing is still done unilaterally from the police to various agencies, from large departments to small ones, and also with large companies that are willing to co-operate with the police. This is counterproductive in the medium and long term. We therefore need to develop a less-restrictive intelligence culture.

A proposed approach would focus on the types of partnerships to be achieved with other law enforcement agencies, based on best practices and major lessons learned. This approach would emphasize potential partnerships with private police services and security agencies used by large corporations such as banks. The approach would further concentrate on opportunities for partnerships with large industries in the area of information technology. These industries are responsible for developing tools for society. It is up to the police to design approaches that are compatible with these tools.

Acknowledgments

I wish to express my sincere thanks to all those who agreed to share their opinions, values, and knowledge in the area of investigations. Without their involvement, this report would have been of lesser quality.

General Introduction

As part of a research program on information technology in law enforcement in Canada, we explored various approaches relating to the emergence and implementation of modern technology within police departments (LeBeuf, 2000a). The police started a long time ago to integrate technology—including databanks such as the Canadian Police Information Centre and many other tools—to improve policing (Soullière, 1999). Also revealed was the fact that the police is currently faced with a number of major changes resulting from the integration of technological tools, the incredible drive toward globalization, and, finally, the constraints stemming from the standardization of work tools, procedures, and methods in general (LeBeuf, 2000b). These changes reflect an inescapable and irreversible trend toward a new paradigm for public law enforcement. We also found that information sharing should now be done with appropriate and compatible tools and that a commitment should be made to conduct serious, recurring budget planning exercises and to update training programs. Finally, we noticed that police knowledge about technological tools, markets, and practices was poor. The police will have to adjust to these technologies at the pace set by the market. Already, experiments in Great Britain have shown that private police agencies and Internet service providers play a leading role in controlling illegal activities on the Net (Wall, 1998). Since one of its roles is to maintain public order, the police needs to use the best means available to succeed in that endeavour. If, as can be observed, social order is changing, the police must keep pace with, and adjust to, this change.

This report discusses two major issues: criminal intelligence and investigative practices in an environment shaped by the emergence of information technology and by a recognized need to share criminal intelligence. We assess, based on available technological tools for criminal intelligence units, including databanks, investigators' concerns about data collection, data entry, and retrieval. We also look at the emphasis placed on data sharing. In addition, we try to determine to what extent the traditional isolation between units, as it relates to investigation practices, contributes to a successful investigation and, more generally, to the successful sharing of data collected for that purpose. We will eventually have to look at the major lessons drawn from work practices in the area of security.

We previously observed that some investigators made limited use of technology. Several factors were identified to explain this situation, including a lack of access to computers and a lack of training on how to operate them (LeBeuf, 2000c; LeBeuf et al., 1999).

The real originality of this research has to do with the fact that, for the most part, it was taken directly from individuals, including analysts, involved in investigations, particularly but not exclusively those on organized crime. We met with investigators, investigation unit managers, and assistant police chiefs in several police departments throughout Canada. We selected members of joint force operations, where several police departments co-operate on an investigation, for instance on outlaw motorcycle gangs, as well as more traditional investigation units, such as drugs, homicides, economic crime, etc. As information technology is being introduced in law enforcement, it is important to find out how this technology is affecting investigators' social practices. A basic premise is that the best source of information, in the general sense of the word, are people who deal with information technology in their jobs. They are in the best position to consider important issues that are sometimes overlooked in the everyday hustle of police operations.

1- Current Technological Developments and Their Impact on the Police

To fully understand the scope of the changes faced by police departments across the country, we need to look at a few transformations affecting Canadian society and the rest of the world.

The evolution and penetration of information technology in society and within organizations, including governments, is proceeding at a fast pace. This evolution is all the more rapid because people are more educated and thus better able to identify their needs, understand the issues related to technology, and make informed choices. Technology creates conditions that are conducive to innovation. Denning (1998) provides a list of some 15 new areas, including intellectual property, distance learning, artificial intelligence, virtual reality, and telepresence. Telepresence opens the door to working at home or away from traditional workplaces. Technology also gives rise to a new work culture (RCMP, 2000).

characterized by a wider and more open flow of ideas, by the use of innovative work methods, such as e-mail, to the extent of being called an "e-mail person," a phrase used by Field (2000), and by temporary one-time alliances for specific tasks. Similar networks are being created by criminal organizations. These advances must not hide the fact that people are facing disruptions because their work practices and habits are being or will eventually be modified. As stated by Norman (2000), it would be better if these technologies remained invisible, as long as people are capable of using them to meet their needs.

In Canada, a two-pronged initiative by the federal government warrants special attention. This initiative is aimed at increasing electronic transactions between all government departments and the community and developing the legislative tools required for large-scale electronic commerce. Let us look at them.

One prong, called Government On-Line and placed under the responsibility of the Department of Justice, is focused on modernizing the services provided to the community. For example, these services will be more direct, faster, and available 24 hours a day throughout the country (see RCMP, 2000: 35 et seq.). The second prong, just as extensive as the first one, deals with large-scale electronic commerce. As mentioned elsewhere (Dryden, 1998), electronic commerce is not new, as funds have been transferred electronically for several years now, although the current development, impetus, and interest by corporations and consumers alike rise to another level. Flowing directly from the concerns expressed by the Organization for Economic Co-operation and Development (OECD), this initiative is aimed at reinforcing user and consumer confidence, establishing basic rules governing the digital market, improving the electronic commerce information infrastructure, and optimizing its benefits (Dryden, 1998). Viewed in the context of the Government's economic agenda, the idea is to foster an expansion of the digital economy, where transactions are conducted electronically (Canada, 2000). The goal is to capture a 5% share of the world electronic commerce by 2003 (RCMP, 2000). To this end, the Government passed the *Privacy Act* (C-6) as of January 2001, which legally recognizes electronic signatures. In this, Canada is following the example of the United States, the European Union, and several European countries (Murray, Vick, Wortley, 1999).

The emergence of information technology gives rise to new threats relating to security and human

activities (Lenton, 2000). For example, the extent to which governments are threatened by information technology through their employees has already been observed. This refers to fraud, computer misuse, hacking, terrorist propaganda, retaliation, etc. (Smith, 1999). It is well known also that cybercrime affects both the law enforcement and business communities (Livanos Cattaui, 1999). After deciding to embrace electronic commerce, the Government will have to make a strong commitment to develop control mechanisms suited to the new procedures in place as well as to the transformation of attitudes induced by technology. This is because every new form of commerce brings with it a new type of criminal activity (White, L. 2000). We could add that it also leads to adjustments to existing procedures. For example, Lloyds of London, an insurance company, is said to be poised to offer its customers a hacking policy (hacking insurance) (White, C. 2000).

The destruction of technological infrastructures is still a real threat and it taken very seriously. The various aspects of this problem were discussed by a task force from the Center for Strategic and International Studies, based in Washington (CSIS, 1998). The list of recommendations alone reflects the seriousness of these issues.

The criminal environment is also changing. After a major investigation on telemarketing involving 951 individuals, the FBI confiscated 92 computers and only three firearms (Robertson, 1999). As noted by Boni and Kovacich (1999), in today's business environment, crimes are facilitated by the criminals' familiarity with the new technology and the information superhighway. The tools required to commit crimes are readily available. Microchips, nanotechnology (Drolet, Moen, 2000), and wireless are all used by the public. What was considered futuristic a few years back is now commonplace.

Internet use, whose growth potential is huge, went from 19% in January 1996 to 60% in January 2000 in homes and other places across Canada. This is a dramatic increase (Ekos Research Associates, 2000). This potential for legal use carries with it a potential for illegal use. Electronic payments are fast, anonymous, and unsupervised because of their large number (Alexander, Munro, 1996), but they are vulnerable to money laundering. The Web provides users with a certain level of anonymity through, among other things, encryption (FBI, 1999) and other software (Scientific American, 2000). It is a kind of buffer that reduces and delays the likelihood of getting intercepted because the evidence is non-

physical and can be easily eliminated (Robertson, 1999; Sullivan, 1999). Furthermore, time and space are irrelevant. Today, it is still relatively difficult to determine the frequency of criminal activities on the Net. They are either not reported or not frequently perpetrated, or law enforcement agencies still do not know how to receive and compile complaints about crimes involving information technology. Today, it would appear that no more than 10% of computer crimes are reported (Davis, Hutchison, 1997). Cybercrimes pose a unique challenge in that they are out of the mainstream of traditional investigation methods used by the police (IACP, 1999).

Several articles provide details on the use of the Internet for money laundering (Sambugaro, 2000), on incredible feats performed by hackers, such as the theft of 300,000 credit card numbers (Organized Crime Digest, 2000b) or 14 and 16-year old teenagers using the credit card numbers of hundreds of individuals (Organized Crime Digest, 2000a), on the expansion of underground banking (Sambugaro, 1999), and on electronic fraud (White, L. 2000). According to a survey published by Deloitte, Touche & Tohmatsu, it would appear that 50% of the largest companies around the world were victims of fraud during their most recent fiscal year. Of those, 25% reported losses of at least $1 million over the last five years (Deloitte, Touche, Tohmatsu, 1999). Furthermore, it is estimated that sophisticated bogus cheque schemes led to losses exceeding US$16 billion in 1998 (Robertson, 1999).

Cybercrime is still hard to define. Here is one way of defining it: Depending on the situation, a computer is either the object or the instrument of the crime (Carter, Katz, 1998). In other words, a computer is involved in, or is associated with, the crime. Currently, cybercrime is viewed in two ways by the law enforcement community. These two approaches are somewhat contradictory. On the one hand, some feel that computer crime as a concept is nothing new. The only novelty is the use of a highly sophisticated tool. With respect to cyberstalking, the following comment was made: "The best way is to quickly shut down your computer." In other words, shutting down the computer eliminates the source of the crime for the victim. This is only a partial solution, especially if the victim works with a computer. On the other hand, others believe that cybercrime represents a new form of criminal activity because it is perpetrated in a new environment. Although burglaries were rare in eighteenth century England because ordinary folks had few belongings, stealing a deer was severely punished (Thompson, 1975). Today, governments and police departments place a heavy emphasis on theft prevention. Both the environment

and the level of wealth have changed. Although cyberstalking is more virtual than physical, its impact on victims is just as real. Hacking is essentially due to a huge increase in the number of computer users. Stealing hardware is also a crime. According to recent estimates, losses from hardware theft reached US$34.7 million between October 1997 and June 1998 (Dertouzos et al., 1999). Replacement costs for these items are very high.

Among the many attempts made to conceptualize cybercrime, one article (TELEMASP Bulletin, 2000) stands out. It identifies five categories. These are not mutually exclusive, but they reflect the new trends in criminal activities.

1. Computers as crime targets: for example, stealing information from a hard disk or intentionally damaging a program or a piece of hardware.
2. Computers as instruments of crime: for example, fraud committed with a computer or telecommunication scams.
3. Computers as accessory to crime: for example, money laundering, electronic pornography, etc.
4. Crime associated with the widespread use of computers: for example, copyright violations, the black market for stolen computer memories, counterfeit equipment.
5. Networking malfeasance: for example, stalking, character assassination through the use of e-mails, and unauthorized access to a computer "just to explore the system."

Wall (1998) suggests another approach: a typology of known crimes. The most widely identified cybercrime groups are "cybertrespass," for instance hacking, "cybertheft," which includes fraud, gambling, etc., "cyberobscenity," which includes child pornography, and "cyberviolence," which includes hate crimes and harassment (see also Sheriff, 1999).

According to Wall (1998), the tendency today is to focus more on the crime and less on the criminal or the victim. One of the senior executives we met made the following comment: "At the present time, there is no feeling that the police is out of step. I think the police knows as much about the Internet as the general population....We can detect the e-mail messages, the hacking. We have no complaints (no. 16)." Yet, electronic mail for one is a widely used tool. Indeed, a 1998 survey of 10,000 Internet or Web users showed that 93% of respondents considered that e-mail has become an indispensable tool

(Boni and Kovacich, 1999).

Some look at how the Net should be policed, but the real question is: How should we investigate crimes associated with technological tools, crimes stemming from alliances between organized groups, crimes committed with traditional means, and finally, an emerging category not yet codified, environmental crimes? Any of these types of crimes may have several of the characteristics mentioned. For instance, the members of various organized crime groups may get together to commit wide-scale fraud on the Web and also for more physical actions, such as intimidation. These same people could be involved in illegally releasing dangerous products into the environment, as is already done (Porteous, 2000). The individuals or groups involved in criminal organizations for economic gains are no longer limited to traditional groups such as the Italian Mafia; they now include groups from more restricted areas (Porteous, 1998). Criminal organizations get involved in cybercrime in several ways, and they are hugely successful at it. According to estimates, over US$10 billion in annual losses are caused by these crimes (TELEMASP Bulletin, 2000). TELEMASP Bulletin 2000 provides a clear and detailed list of 10 activities ranging from the black market to virtual gambling, to illegal immigration, to telecommunication scams, to sexual trade, and to identification theft.

With these new types of crimes, new social prevention measures will be required (United Nations, 1999; Parsons, 1998), and new security approaches will have to be developed so that, in the words of Blackburn (2000), "thieves that use their eyes instead of a weapon" to get your credit card number can be tracked down. Two actions taken recently are worth mentioning. In February 2000, more than 150 organizations from 28 countries, including American federal agencies, attorneys general, consumer protection offices, better business bureaus, the Hong Kong Consumer Council, and the University of Texas Law School, under the sponsorship of the Federal Trade Commission's Bureau of Consumer Protection, patrolled the Net to identify questionable trade practices. More than 1,600 suspicious sites were identified and advised that law enforcement agencies would be informed of their activities (The Report on Crime and Profiteering, 2000). Furthermore, the President of the International Marketing Supervision Network, an organization made up of law enforcement departments, government agencies, business offices, and individuals from 29 countries, whose mandate is to fight Internet fraud, recommended that the various pieces of legislation on consumer protection at the national and

international levels be shared and updated (Organized Crime Digest, 2000c). It should be pointed out that the required actions are not taken only via the traditional criminal prosecution route, but also through civil law. In addition, these two examples are a direct demonstration of the existing co-operation between law enforcement and other interested parties not normally invited to work with the police.

The recently published literature contains scores of articles on the major issues relating to investigation methods used for crimes involving information technology, such as computers (see, among others, Icove et al., 1995; Osterburg, Ward, 1997; Mendell, 1998; Richards, 1999). The increasing importance of this type of crime was demonstrated when Janet Reno, the United States Attorney General, provided substantial funding to analyse the complexity of this phenomenon and to develop suitable training programs (USA, 1999; Williams, 1999). In our situation, given that one of the priorities of the federal and provincial governments is to fight organized crime, it appears that two major issues intersect:

- generating intelligence and information to develop effective strategies
- understanding and recognizing the technological tools used by the community, the criminal world and the police.

The examples above make us realize that investigative practices have already started to change, and this process will surely continue. The selection and training of investigators need to be reviewed right away. The speed, ease, and apparent lack of traditional barriers that characterize this type of crime are a reminder of how easy it is, for example, for an individual living in country X to defraud an institution in country Y through a server located in country Z. That is the real threat.

The question is therefore how to conduct an investigation when information technology is involved in the crime? This question is especially relevant in terms of the investigation practices used in the field given the significant changes occurring to organized crime in Canada. Organized crime is one of the priorities of the RCMP. Likewise for the Federal Government and the various criminal justice partners throughout the country. In October 1998, a Joint Statement on Organized Crime (Canada, 1998) was signed by the Federal, Provincial and Territorial Justice Ministers. It contains a commitment by the Federal Government to provide national leadership "by fostering cooperation between law enforcement agencies, the private sector and various community groups".

2- Investigative/Criminal Analysis, Practices, and Procedures

Investigations are recognized as a unique activity within law enforcement. Investigators work in civilian clothes, sometimes wearing only a pair of jeans and a T-shirt. They have flexible working hours, which are in fact adjusted to the requirements of surveillance and intercept operations. They have some latitude in the approach they use, depending on the type of crime being investigated. They are also responsible for compiling information, analysing intelligence, and finding leads in their fight against crime.

In the field of investigations, as elsewhere, work habits and learned approaches die hard. After basic training, continuous development, and on-the-job training, "giving up old habits" is not easy (no. 11), as was mentioned. Improving our response to organized crime based, among other things, on the use of JFOs and an encouragement to collect information for storage in computerized databanks has less to do with fighting this type of crime than with the cultural change required to achieve results. In other words, it seems less important to launch a crusade against organized crime than to get police departments to co-operate. Even though there is an immediate willingness to do this, the fact remains that cultural irritants persist. "The biggest problem is to get the guys to work together" (no. 18). It is as much a matter of developing a shared vision and common objectives as identifying how each member can help reach preset goals. There is also a deep-seated reluctance regarding accountability in an environment where it would be normal to take calculated risks. As was explained to us: "Risk management is more the management part than the risk part" (no. 2).

In a changing and evolving environment, available technological tools are not used systematically by police officers and investigators. Three comments are in order:

First, it would be incorrect to say that the use of technology is related to age, that younger officers are more likely to use it than older ones (both in terms of age and seniority). "We can't generalize. Some young guys fear technology, while older ones, with 25 years of service, enjoy it" (no. 5). Also: "Officers that are both computer-literate and experienced are a cut above the others. Our most senior member, with 32 years of service, got interested in computers fairly late in his career, but he soon became a real wizard. He was interested in everything. He even trained us. He developed computer use during the last

four or five years of his career" (no. 19).

The second comment relates to an adjustment period associated with the introduction and use of technology. Experiencing some difficulty when using a new software, a new computer, or an upgraded databank is perfectly normal. This period, which may last a while, is described as an unnecessary waste of time (no. 12), whatever the position may be within the organization. Individual or formal training, support, help from co-workers, and the use of a keyboard to enter data into a computer are also considered to be a waste of time. This is reflected in the following comments: "Technology is taking us backwards. Asking us to bang away on a keyboard is a waste of time" (no. 15, 14); "You spend half your time trying to figure out how it works electronically. You get to keep relearning new things" (no. 3). Another comment: "Playing with a computer is like a hobby. I invest my own personal time to learn" (no. 17). Finally: "I spend a lot of time helping colleagues find things. We learn from each other" (no. 25).

The third comment flows directly from the previous one. Although an adjustment period is unavoidable and probably required, appropriate solutions are implemented downstream because they were not included in strategic planning to partially address an issue considered to be very annoying by police officers. We were told that "more and more specialized units are being created to help not only in understanding technological tools, but also in using them properly." We also picked up this comment: "A section is assisting us with data collection during searches" (no. 12).

2.1- Crime Investigation Practices

For first line police officers, the emergence and use of databanks, such as the Canadian Police Information Centre, has helped improve traffic law enforcement. These tools have also enhanced the performance of police officers. On the other hand, the benefits of high-performance technological tools for investigators and managers are much more questionable. Benson (1993) reminds us, for example, that the introduction of the Home Office Large Major Enquiry System (HOLMES), designed to set standards for information collection and compilation, failed to solve most crimes in Great Britain.

For investigation and analysis purposes, information technology is still perceived as new and threatening. Indeed, it was described a few years ago as a "collection of gadgets" by an investigation unit manager. Some are still wondering who should use this technology and which investigators should have access to it, especially in the area of cybercrime. As previously observed, the emergence of information technology in law enforcement is somewhat inflexible and rarely planned. Police officers deal with criminals who have a better grasp of computers and technology. Police officers also lack adequate and timely training. Because their skills and training are found wanting, they have to rely on outside help from specialized companies or on in-house experts. Furthermore, technological advances are occurring so fast that police officers are finding it hard to keep pace. A shortage of equipment or adequate equipment and the amount of time needed to conduct thorough investigations were also mentioned (LeBeuf, 2000a, 2000b).

All sorts of consequences at various levels flow from this. The first major one is that the police environment should have been prepared to deal with these technological advances before police officers, investigators, and analysts were asked how they used the available technology. Yet, this crucial familiarization period is either dismissed with comments such as, "That's a great toy (computer)," or it is misunderstood, in which case technology is seen as a threat that can only be dealt with by experts: "Investigators are blinded by their fear of technology..." (no. 19).

A second consequence is directly linked to the proper use of technology. Here again, significant and unavoidable changes to police practices are too often ignored because of a lack of preparation. An interesting comment was offered on this topic. A manager noticed that several investigators made little or no use of the available computers to write their reports and their search warrants: "The guys write their affidavits by hand because they are not familiar with computers. The copy and paste function is not mastered by everyone. The copying and pasting is done by hand and it is given to a secretary" (no. 13). Another manager commented on the same topic: "I want them to learn how to use computers. I don't want these reports done at home by their wives. Changes are coming because they're going to have to sit down and enter their data into computers..." (no. 4).

It is generally recognized that a real need exists for these technological tools. As was rightly stated: "The

Hell's Angels have e-mail and Web sites. We need them too" (no. 10). Responding to this need is still partly dependent on access, on easy and immediate access. Some would say "user friendly" (no. 26). Many investigators said they did not have their own workstation. According to the unit, the ratio is four to six individuals per computer. "We don't have enough computers. You have to wait your turn, which may take one to two hours" (no. 22). However, an organization like the RCMP provides its investigation and analysis staff with all the equipment they need.

It follows that investigation and analysis practices are directly affected by this. In fact, direct access leads to practices where using a computer, and hence a computerized databank, become systematic depending on the section involved. The opposite is also true. "Here, the use of technology is developing slowly....In my previous job we automatically checked the databanks. Here, we don't" (no. 9).

A JFO manager discussing the technological tools available to his staff mentioned that no one had a personal computer. He said: "My job is finding evidence that they (members of organized crime) are involved in drug trafficking, not playing with a computer....If you need any support to collect your evidence, do what it takes to get it" (no. 7). This reflects in part the hurdles investigators face daily when dealing with technology. For example, a member of an economic crime unit revealed that he was the only one with any expertise in the understanding and use of information technology: "I was the only one capable of storing my evidence electronically, i.e., an 80,000-page document with annexes on two CD-ROMs. That was a first in the economic crime unit. We scanned the hard copies, and hyperlinks are possible. My investigation notebook is now computerized. Before, everything was done by hand. It has been in a computer for three years" (no. 5).

Personnel and skill development, including for investigators, is now part of the evolution of the police. These skills are particularly critical in areas related to technology, where officers readily recognize that they are not capable of investigating, either because they are unfamiliar with the technology involved, such as the Internet, or because they are unable to measure its impact. Their arguments are expressed like this: "For emerging crimes, we are not equipped or trained, and we don't have the required tools. We are missing a lot of things, and we criticize" (no. 21). Also: "We are not ready to work on them. We lack the skills necessary for this type of investigation" (no. 22). Further: "With cybercrime and e-

commerce, if we stay within our jurisdictions we'll never manage. It's awful. We must use a more comprehensive approach" (no. 5). As can be seen, expertise is a must. Yet, the development of advanced skills creates major problems for the police because of staff mobility. The way the promotion process works, even highly qualified individuals must leave their area of expertise (there are exceptions) when they are promoted. When these individuals leave their jobs, there is a loss of expertise. Those who quit to join the private sector and the often lengthy period of time required to fill the vacancy should also be taken into account. For a manager, "personnel mobility is the biggest problem. There is a loss of expertise, and finding someone to fill the position takes time....I won't get a replacement for five months..." (no. 4). A JFO manager stated: "We lose those who are promoted. We can't keep our expertise" (no. 7). Also: "Police officers are rotated all the time. We need more stability" (no. 17). With the development of cutting-edge specialists, there is a complete loss of expertise when these people leave. An expert discussing his job made the following comment: "I'm the only one with contacts. When I'm no longer there, all our contacts will be gone. The lack of a central drop-off point is a big problem" (no. 19).

One unexpected consequence of the emergence and use of technology is a new work distribution. It is not so much the type of work that is changing as the workload and the extra steps required. The steps relating to data collection and storage (in databanks) are what seem to add to the workload. The following comment was made on this subject: "With technology, we're not efficient. Our work should be more efficient, but our workload is increasing" (no. 15). Also: "Less and less people are asked to do more and more" (no. 19). Finally: "Police officers do computer processing day in day out. It's a total waste. We need civilians to do these jobs"(nos. 14, 30).

What does the future hold? Some talk of virtual patrols on the Net as practiced, although not exclusively, by the FBI, the US Secret Service, and the Customs Service by comparing traditional street crimes with computer crimes (Sullivan, 1999). In some police departments in Canada, "Net surveillance is already an option" (no. 8). Others recognize that they tend to use the software applications and tools they know best and have no desire of familiarizing themselves with other tools. Yet, this field is evolving at a very rapid pace. "We work with the software applications we're familiar with....Some are used as

tools to improve and speed up the management process...but the investigators reacted negatively" (no. 5).

In short, it would be incorrect to say that the use of technology is related to age or seniority. It has to do, above all, with the development of the right attitudes. Furthermore, it is only normal that individual learning, program training, and assistance to co-workers would go through an adjustment period. This period is seen as a waste of time, as a loss of job efficiency. Finally, increasingly sophisticated specialized services help police officers carry out tasks such as capturing data from hard disks.

A lack of preparation of the law enforcement community to the emergence and partial implementation of technology has led to specific consequences, such as denying the adjustment period required after the introduction of tools that were completely new to the police. Another consequence is forcing individuals to adopt new practices without proper training.

Investigation practices are affected by the availability of technological tools such as computers and by the underused potential of devices such as CD-ROMs. We need not only to arouse the curiosity of individuals but also to support their development.

Finally, the police is constantly faced with the need to provide new training to its personnel because individuals have to leave their field of expertise when they are promoted.

2.2- Investigation Methods

If, as we contend, investigators generally lack vision when conducting their investigations, there would appear to be a need to look at how they perceive their jobs. We focused mainly on the traditional isolation that exists within the investigator community because of the creation of various units to conduct investigations in a more efficient manner. The existence of separate units such as the economic crime unit, the homicide unit, the drug unit, etc. impedes contacts between police officers for either traditional or cultural reasons. An investigation unit manager summarized the most traditional approach to

investigations this way: "Understanding the nature of a crime is easy; proving it is something else altogether. If investigators are provided with all the tools they need, they will achieve real results" (29).

Three findings are obvious. The investigation community seems to be suffering from a quick action syndrome. Computerized research methods based on various software tools are still not valued. As stated by the head of a major investigation unit, "Investigators fail to see the need to search through databanks....You won't find offenders in there" (no. 13).

The investigation community can't keep pace with criminals. Otherwise, "it would have changed over time, just like organized crime has" (no. 22), but it hasn't. One way to correct this situation would be to start an investigation by analysing available intelligence to structure a proper strategy. It is said that too often "things start at the bottom, with investigators following a lead and thinking they will eventually get to the king pin....This is a real waste of money" (no. 15).

Police officers can now use technology to conduct investigations and to collect and manage information. When investigators submitted evidence on a DVD, there was a positive reaction from the judge, the prosecutors, and the defence attorneys. Since then, "we've seen an increase in the number of requests to submit evidence in this manner, especially in major cases" (no 8). Ironically, both investigators and analysts recognize that "investigators in general are not very adept at, or much interested in, structuring information with these tools...But they can learn" (no 24). However, more and more investigators will have to deal with real-time technology in the near future. They will also see the scope of the problem resulting from the disappearance of borders while laws still have to be enforced within national jurisdictions. Finally, a day will come when within the framework of a regular investigation, the traditional part and the technological part will have to identified: "We must be able to investigate, to get the major pieces without getting involved in technical stuff" (no. 19). This is one of the biggest challenges facing the police.

The investigation units as presently structured tend to isolate the members. Several said that this isolation is necessary and, furthermore, that it should be maintained as it is. Their arguments are that required

resources, investigative skills, and relationships with prosecutors are specific to particular types of investigations. "Resources are not the same for homicide as for drug investigations. Each area has its own specialties, Crown prosecutors, case law, etc." (no. 4). Also: "Each investigation has very specific things" (no. 20). Overall, it is generally agreed that "there will always be a need to develop specific expertise for drugs and other crimes and to provide services to each one" (no. 11).

Building and maintaining expertise in conducting investigations is critical for several basic reasons. In fact, expertise equals skills in conducting investigations. As previously noted, "We live in a world of specialty....The courts have been making such voluminous decisions. There has been so much case law and so much new development and interpretation in the last 15 years, it has forced police forces to have specialists. So they say you can focus on homicide because it is your specialty and you are really good at doing homicide....If you can't carry your specialty, your team will fail" (no. 27).

Similarly, a lack of expertise or a "generalist approach" would amount to a lack of skills. To quote an investigator, "Generalists are less skilled. You know a little bit about everything, but nothing in depth....Having specialists is important" (no. 17). This opinion was shared by several of those interviewed, who noted that in this day and age, investigations require "specific and highly specialized skills. An investigator can't be good at everything" (no. 13). Furthermore, these skills are required because of the development of legislation, such as the *Canadian Charter of Rights and Freedoms*, and case law, which make investigations more complex and more demanding. It is critical that "people be allowed to develop an expertise and broaden their horizon at the same time" (no. 1, 3). There are also international investigations requiring advanced expertise and specific skills. Fighting transnational crime demands new skills. "Today it is transnational. So in order for an investigator to be effective, he needs to learn not only about the laws in Canada, but also about those in China, etc." (no. 3).

In the field of investigation, crime analysts are a special category of expert. There are two types of analysts: civilians (civilian members and civil servants) and police officers. The advantage of using the second type is said to be that "it is easier for a police officer to understand the procedure through the language used" (no. 6). Its disadvantage is a high rotation rate among police officers, as an analyst's

position is a "springboard to other things within the Force" (no. 24). The overall opinion of analysts is that they are part of the investigation process. Several analysts are civilians, and they are said to create "a momentum that helps investigators move forward because, among other things, they think differently than police officers" (no. 1). It is also said that they make a special contribution. This contribution may be different depending on the type of investigation they are working on. First, they are said to structure "investigation files so that they can be brought to court" (no. 8). Using software, they create hyperlinks to data, and these links could not be made by investigators who "know nothing about technology" (no. 23). "They are unable to do it. They collect the information, they bring it to me, and they tell me to do it" (no. 6). They also cast a different light on investigations, which sometimes makes it possible to redirect things based on new information (no. 25). This contribution may also affect the direction taken by the investigation. One analyst said, "Analysts tend to be in charge of investigations. You tell the investigator where things stand, always relying on available information" (no. 6). Lastly, it appears that analysts are not concerned with information sharing. They feel they have specific areas of expertise that are not conducive to making contacts and sharing information (nos. 23, 14).

However, the need to work in isolation and with experts creates specific problems. For instance, working in this manner fosters competition between units within the same department (no 16). Some units seem to have a better situation, at least a higher profile as seen from the outside. This creates a real problem in terms of the expertise developed within the unit: this expertise could be lost when individuals are attracted to more "prominent" units. This competition is also reflected in the day-to-day processing of investigations. If, for example, a connection is made to organized crime during an investigation, investigators will say that they will make the necessary links and will contact their colleagues. "They will be given different leads" (no. 12). But it appears these contacts will not be made systematically. The real issue that is not being considered seems to be "Who will take the case if the homicide unit is no longer there?" (no. 6). In other words, which unit will assume formal responsibility for the investigation and its results?

Is there an informal ranking of police units? The answer to this question is definitely yes. The reasons are extremely interesting. Some crimes, it is said, can be used to the maximum. "Some types of crimes lend

themselves more to this, when there is a lot of blood, a lot of publicity....You don't see the same thing throughout law enforcement" (no. 9). In addition, as noted by an investigator in the area of operations, "skills are measured against results." This attitude, which may be questionable, creates a sense of urgency and leads to specific responses. In fact, some units cause envy because of their high-profile activities. "Management is aware that organized crime investigators move faster and do more overtime hours. They have bigger budgets because they go after big catches" (no. 16). Some feel that JFO members are trying desperately to make their actions public, thinking that this kind of publicity will yield benefits such as higher budgets, cell phones, and computers for everyone. Someone said, "They have more money, there is a lot of rivalry" (no. 14). Also, "Individuals from these units tend to shut out the others because they want to be in the spotlight" (no. 22). Conversely, members of units that have less publicity are seen as less important and are less likely to attract new teammates. Hence this comment: "In economic crime, we take whoever wants to come, whereas in personal crime, we take whoever we want" (no. 17). The following quote from an economic crime unit investigator is reflective of the situation: "Internally, we're seen as paper shufflers, away from the action. Externally, we're seen as professionals" (no. 4).

In short, there is a real and necessary isolation between investigation units. This results from the development of an advanced expertise to meet specific investigation problems.

This isolation creates competition among units, which in some cases has a strong public impact. It also fosters the development of cutting-edge skills in specific areas.

Analysts are a separate category of investigation expert. Investigators need them. Their contributions include managing complex information, providing direction, and understanding the various elements linked to an investigation.

There is an informal ranking of investigation units, which has consequences in terms of publicity, budgets, and technology such as cellular telephones, computers, pagers, etc. for members of these units.

The investigation community—a key law enforcement community if ever there was one—accepts the required changes at a snail's pace. Investigation methods would be better if a dynamic approach were used, where various elements were involved both in the traditional ways of doing things and in other more innovative techniques. This approach suggests that there may be ways of conducting investigations that are more relevant or better suited to the current criminal environment.

2.2.1- Crime Response Joint Force Operations

Crime response joint force operations are a particular type of investigation unit. JFOs are made up of members from various police departments and, if required, law enforcement officers from agencies such as Customs and Excise Canada, etc. The goal is to combine forces, for example, to fight organized crime. This type of concept grew out of three basic, interconnected, but not always well-defined findings:

- "A single police department can't fight crime alone." (no. 11)
- "Some police units too often work in isolation without using the resources and information provided by others." (no. 7)
- Funding is important; however, few governments have new money to invest. (no. 7)

JFOs are not a new phenomenon. For example, joint units set up by the RCMP have been fighting drug trafficking in Vancouver harbour for at least 15 years. This concept is now growing. Some JFOs are permanent while others are more of a one-time effort. Joint units such as the Combined Forces Special Enforcement Unit (CFSEU) (Hamilton, 2000) are used to fight organized crime in the Toronto metropolitan area. Also, police intelligence units made up of investigators and analysts are combined for intelligence purposes. Partnerships with large corporations, e.g., with Canadian National or the banking industry investigation sections, are also contemplated.

At least three contributing factors have been identified. First, JFOs are described as a new police approach in this sense: As various police departments "sit around the same table," their efforts are combined (nos. 20, 10, 30). "I always found that JFOs are the best way to go" (no. 28). It should be

pointed out, however, that this combination of efforts causes a number of problems related to work habits, basic training, continuous development, working conditions, work schedules, supervision policies, and budgets. On the other hand, it leads to a better co-ordination of response options, investigative approaches, and budgets based on specific goals. The real driving force is less the individual and more the organization. Some say that joint actions have the added benefit of broadening the perspective and concerns of a number of police officers (no. 1). For the time being, the cultural values of each department are the real challenge.

The second contributing factor is that joint force operations are now considered to be the preferred solution for twenty-first century policing. "Multidisciplinary teams made up of experts from various fields of investigation are the best way to go at the moment. They bring together people with different backgrounds and specific skills in various areas....These teams are a modification of the old ways of doing things. They are a departure from specific warrants: their response is not based on a warrant, but on a group" (no. 29). Rallying parts of law enforcement provides relatively effective one-time alliances (no 2). With this type of partnerships, individuals are less concerned with their own sphere of influence (turf) and more focused on the target. Furthermore, as a result of a combination of various departments, help for specific operations is easy to get and quickly obtained because of existing formal contacts (no. 14). Ultimately, the police becomes more efficient as there is no duplication of energy and effort in pursuing leads.

A third factor, already mentioned, is that JFOs provide response options that, when combined under a single banner, help units or sections that have neither the time nor the equipment to act on their own (no. 6, 11). In addition, police officers from small and medium-size departments benefit greatly from this type of integration as they learn from being in contact with various procedures, work techniques, and problem-solving approaches and also from the clash of cultures. Furthermore, this creates a spirit of co-operation between individuals, regardless of their background, thus providing added value to the police (no. 23).

A number of disadvantages that, according to some, impede the success of joint force operations also need to be mentioned. At least two were identified. The first involves individual skills and knowledge. In an environment with complex legislation and procedures, it is obvious that individual skills are not all at the same level. Not only is the training different, but developed skills are not always on a par either: "The partners are excellent, but their training is very different from that of peace officers" (no 14). In addition, where there is fear that "the big guys (departments) will dominate" (no. 2), past experiences and developed skills have an impact at several levels, including on small departments. Complicated procedures, investigation philosophy, and reporting structures are factors that may make a unit less effective than it might otherwise be (no. 14). Finally, there is always the potential of a rivalry developing between members, in which case the project could be in jeopardy. Hence this comment: "You can lead a horse to water but you can't make it drink. You have to convince people that it is the right thing to do" (no. 27).

The second disadvantage has to do with unit management. Viewed as a structural problem, it is a matter of determining how a manager should build a real team where all members are focused on the same goal. "It goes to the personalities of the team leader....If he can, it will work relatively well. If he can't, then that is where problems start to..." (no. 3). This issue also has to be looked at in a context where individuals from member units do not report to the team leader for their annual assessment, annual leave, etc. "None of them is answering to you for performance review, assessment, or anything. You may have a say if the supervisor asks. The team leader has responsibility for the day-to-day" (no. 14).

In short, joint force operations appear to be an effective and relatively new crime-fighting tool. They make it possible to combine investigation options, budgets, law enforcement tools, and individuals to achieve a common objective. They also prevent force overlaps in an ever-changing environment.

JFOs also foster one-time alliances and valuable contacts between individuals and organizations. As a result, requests for assistance are much easier.

Impediments to achieving a unit's expected effectiveness include differences in cultural values between organizations and issues such as benefits, complex procedures, investigation philosophy, reporting structures, work habits, basic training, continuous development, working conditions, work schedules, supervision policies, and available budgets. On the other hand, a major element is information sharing.

3- Intelligence and Its Uses

The information contained in computerized databanks or police files is used as an investigation tool. Current intelligence will identify the best targets for effective police operations. It therefore becomes important to know what purposes are served by compiling this information, especially when fighting organized crime. This question reveals a lack of consistency with respect to the goals to be achieved. This inconsistency could suggest that the differences mentioned below may be explained by deficient training programs, a lack of adequate training, or simply the unavailability of training.

Given that one of the prime movers for this research is organized crime, we feel compelled to highlight some perceptions voiced by the people interviewed. One individual provided an accurate picture of the situation: "When you use the word organized crime, the definition itself means different things to different people depending on who you're talking to: the business community, the general community, small police departments, large police departments, the banking community. It has a different face for everyone" (no. 2). Because of the difficulty of agreeing on a simple definition for the whole community (no. 2), planning and updating the fight against organized crime give rise to complex issues. For instance: "If you focus on something based on criminal intelligence, you're bound to overlook something else. Concentrating on motorcycle gangs means that Aboriginals, Italians, Eastern Europeans and Jamaicans will move in. If we keep going in one direction, new problems will appear, and this will indirectly force elected officials to recognize that we don't necessarily have all the tools required to fight organized crime" (no. 1).

A further comment: "Organized crime is a juicy target. It sells" (no. 4). Also: "With organized crime, the attitude is I have an informant, I have good information, I pull out a search warrant, I break through the door, and I charge someone. These people don't care about paperwork" (no. 5).

There is also a sense of uncontrolled fear and dread by the police. This fear seems to be based less on solid information and more on perceived common sense. For instance, some said, "They're well organized. They're everywhere The more you look, the better organized they are" (no. 10). Furthermore, "We're overwhelmed, concerned. Police work is very expensive....We're not on an equal footing, we don't have the same budgets or the same rules" (no. 9). Also: "The procedures for evidence disclosure are becoming more complex, and, besides, they're known to the offenders (no. 12).

3.1- Purposes of Gathering Police Information

According to interviewed investigators, there are as many reasons as there are priorities. We divided them into three mutually inclusive categories. Before discussing them, however, let us look at one of the findings regarding collected information: a majority of interviewed individuals agreed that collected information is an investigation tool. "Info. is a tool to get business done" (no. 3). Even when not precise, information provides direction to investigators. For example, one investigator noted, "Info. is dry. It's used for investigations. It provides good leads on individuals. After you're posted to a new detachment it takes you one to two years to know the people. If a databank had been available, you could have tapped away to get the background of everyone that worked here before you" (no. 18).

Now, let us discuss the three categories.

The first category is that information is used as a guide to provide directions either for the investigation or for the officers involved. It may, for example, show vehicle usage or identify individuals or prior offenses and investigations. If the information is current, it can be used in a case file. Having observed that "not everyone benefits from getting information" (no. 16), someone added: "When you initiate an investigation on an individual to find out what has been done, you have the opportunity of contacting the investigators

that were previously involved. The larger the department, the more it benefits from intelligence" (no. 16). In this sense, information is not used to "execute a warrant, but to find out if you're on the right track" (no. 13).

Others felt that "as information becomes available, the officers can make sound and solid decisions" (no. 1). But, they added: "they don't have access to the information at the moment." The impact of these decisions would be to get police officers to focus less on individuals and more on groups or organizations to which they belong, especially for members of organized crime (no. 3). Actually, the investigation culture is what needs to be reconsidered. We will return to that issue later.

The second category is that information enhances the quality of operations, helps design a strategy, and supports in-depth analyses. By stating that "information is power," an investigator emphasized that intelligence "helps reduce bottlenecks and identify leads: location, time, etc. It actually helps the police stay one step ahead of criminals" (no. 7). Indeed, if information was used as part of a well-planned strategy, statements like the next one would not be relevant: "The Hell's Angels, why is it that they continue to function? The answer is when you look at the way we are establishing our priorities, they are being driven by informants on the street" (no. 30).

The third category is that information is used specifically to write affidavits. As stated, "You know what it takes for an investigation to go to court" (no. 6). Information meets the needs of investigators and analysts in preparing adequate cases while complying with existing legislation.

In short, as can be seen, information helps the overall investigation by documenting case histories, directing the pursuit of more targeted leads, and, finally, facilitating the preparation of court documents. This information is assumed to be current and of high quality.

However, the quality and use of this information are yet to be determined. Let us now look at these issues.

3.2- Quality and Use of Information

Interviewed individuals generally agreed that the information collected in case files and databanks is "significant and meaningful" (no. 1). This information must be usable, i.e., reliable and, most of all, current. Currency of information depends on the direction of the investigation. As stated by a manager, "It's not accurate to say that information benefits everyone. What is true today might not be true tomorrow, and vice versa. Everything in a databank is true even though it might not be usable" (no 16). Yet, what is important is that investigators get access to the information and that they are capable of interpreting it, which seems to be a real problem. Indeed, databanks facilitate police work to a certain extent, as long as officers are capable of adequately handling and interpreting this information. A specialized investigation manager rightly observed, "It is one thing to collect it. What you do with it, how you make use of it as a broad picture, I guess, is the real question" (no. 3).

This comment refers directly to the probative value of information, a value that, for many, should be the basis for specific actions such as arrests, convictions, and evidence submission.

"Collecting intelligence is all well and good. But, what type of information? Can it be used as evidence? Can it help make arrests and get convictions?...The value of intelligence is real in that information equals results. Although some information has no ultimate result...it's difficult to measure the actual value of such information" (no. 7).

In addition, even with the large amount of available information through multiple national databanks and local police department databanks, there is a need to continue supplying information to these banks because "often critical elements are missing....Really key info. does not get into the system....To filter it out together and to link the events is what is really missing....How do you put it together so it makes sense for your purposes?" (no. 3). At least two reasons are given to explain this situation: "We do not have the particular skill sets around, and also because our technology has overloaded us with information" (no. 3).

Similarly, a lack of co-ordination between systems and, incidentally, between police departments is a major reason why information quality is deficient (no. 14). Uncertainty about the reliability of the information is also an issue: "There is too much that I can't disclose or that's of no use for me...." So an investigator decides to close his or her file. Due to a lack of time and a heavy workload "you close your file, otherwise this could go on for ever" (no. 5).

Finally, this information is sometimes used for secondary purposes, such as public relations through the media. Some said that the information is then used, for example, for "bragging rights," to show that the police department is the best. This breeds a certain "resentment that someone used my information to strengthen his ego or enhance his image" (no. 8).

In short, an emerging concern is that a more comprehensive collection of information should be encouraged. It is not so much a matter of collecting information as collecting quality information. Also, quality information leads to specific actions such as arrests and convictions. Where possible, the information should be current and reliable. Finally, it appears that information can be used for secondary purposes such as bragging rights for police departments.

3.3- **Information Sharing – Myth or Reality**?

One should be skeptical of the claim that this concern about information collecting and sharing has been the same since at least the sixties. This attitude shows a misunderstanding of the broad legal (legislation and case law) and cultural changes that police officers and departments have had to deal with. There are also factors related to budgets and to available and rotating personnel. We will discuss these factors later.

Information sharing is in itself a fundamental problem for the police. It depends on co-operation among members of a police department and with other departments across the country and around the world. At a time when information technology is growing by leaps and bounds and is making real-time

communications possible all over the world, the real question related to the sharing of police information needs to be asked.

What are we talking about? What is to be shared? The answers to these questions are not always clear. It could be general information, partly analysed intelligence, source or informant reports, etc. Note that the same level of sharing is not required for all investigations (no. 13), and it is not necessary to share everything. Therefore, how can we separate what needs to be shared from what does not, and how can this be encouraged?

As a result of our meetings and observations, we feel we have uncovered a few unquestioned **stereotypes or conventions** concerning information sharing. They circulate in the investigation community and in the police in general. We list them below without discussing them.

1. Information security, individual trust, and work methods depend on the need to know as compared with the right to know.

2. Police officers keep their information for themselves. They only put part of it in case files or databanks.

3. Investigators are generally overloaded. They don't have enough time to manage huge amounts of information because of the administrative work (preparation of warrants) required by the legislation and case law.

4. The more information the investigators have, the more successful the investigations will be.

5. Any refusal to share information is above all a management problem. In other words, these refusals sometimes look like political squabbles.

6. A refusal to share information is a direct consequence of a lack of co-operation between the police officers involved. They fail to do their part once the formal agreements have been signed at another level.

7. Information sharing depends more on the willingness of individuals than on the implementation of administrative policies.

These stereotypes take root in investigation practices and learning. They also reflect the stigma of past situations that have left scars that are difficult to heal. As noted by an investigator, "When it happens, scars remain for a long time" (no. 24). We will now look at factors related to information sharing and non-sharing.

All contacted individuals agreed right away, each in their own way, that information sharing is important in principle. Sharing is subjected to a series of formal and informal factors to protect the information, the investigators, the information sources, and the investigation itself. Depending on the situation and the investigation, the information is sometimes not shared within an investigation team. Naturally, in such instances, the information would not be provided to other members of the police department or to other departments in Canada or abroad.

Ultimately, although information sharing is advisable in principle because "when information is exchanged, organizations avoid overlaps between them" (no. 9), a series of factors contributes to the non-sharing of information.

3.3.1- Non-Sharing Factors

At least four sets of factors were identified. They are listed and discussed below.

The first set of factors is related to mutual trust between individuals and partners. Trust has to be created and developed between individuals and organizations. It must be supported at all levels of the

organization so that a trusting relationship at one level is not undermined by individual actions at another level. Generally, when there is a lack of trust, which seems to be the general rule at the outset, individuals are reluctant to give anything (no. 26). Trust must also be the basis of relationships between investigators and their sources or informants. However, the trust that characterizes police-informant relationships can be lost if the relationship becomes known. "My contacts, my sources...the bond of trust would suffer if everything was disclosed. A level of professional discretion is also needed; one could say: I'm willing to help but there are things I won't disclose" (no. 21).

Furthermore, investigators often obtain privileged information or have access to databanks belonging to police departments that are part of the same joint force operation because they have made contacts and enjoy a credibility that help them manage their cases effectively. If they leave their position or are no longer a part of the JFO, the information flow stops immediately.

A second set of factors concerns legal issues. Information is sometimes provided by third parties to help move an investigation forward. But a time comes when the organization has to inform its sources that it wishes to use some of their information in a formal investigation. The third-party rule would then apply, which means that neither the information nor the sources may be disclosed in an affidavit if the third party is unwilling to do so. Also, privacy protection and access to information legislation is designed to control or rather circumscribe information sharing and protection rules. Finally, sharing information with international organizations is an emerging and crucial issue. Law enforcement jurisdictions and practices are different. The real unanswered question is this: Who will share information with international agencies? (no. 11)

As for individuals, police authority set out in the constitution motivates them to contact the RCMP to give information. "If someone gives me something that belongs to the RCMP, I feel I have to share it with them" (no. 13).

The third set has to do with investigation work methods. This set is complex because it includes personal attitudes, methods learned on the job with colleagues, and a lack of familiarity with how computer systems work. Let us look at each of these items.

It has been observed that investigators who disregard their information sharing responsibility do not really know how to work strategically (no 11). "We still do not get the intelligence. The drug people are not sharing their info. with intelligence people; none of them are sharing their intelligence with the intelligence bureau CISC" (no. 28). Maybe they have not learned to do it, or maybe they fail to see the need for it, which is even worse. In this case, the rationale, which comes under attitudes and professional culture, is that "people don't talk to each other—it's human nature. They protect their own turf in their professional dealings" (no. 15). Sharing information would mean they are losing control over their own work (their investigation).

On the other hand, several stated that information in general is power. Information therefore becomes some sort of "exclusive preserve" of "things you don't want to talk about" (no. 22). Also: "There is a certain percentage of investigators who are very proprietary, protective, and selfish with their info. I think it is a minority" (no. 27).

Added to this is that information sharing problems are, for some, a matter of trust between the police and the information sources. "When meeting sources, we often build relationships based on trust. They give us information with the understanding that we will keep it to ourselves, that we won't share it with anyone else" (no. 13). In other words, these individuals are willing to talk to investigators as long as the information is not passed around. The very reason for getting the information becomes an obstacle to sharing it. Trust develops. It is based for the most part on the need and right to know. For some, however, "the need to know/right to know has been abused for years and years. If we would sit down and analyse in some way the most stuff that could be shared, I would like to think that it is only the very small stuff that is so sensitive that it has to be protected in some way" (no. 28). This comment suggests that the approaches and especially the attitudes toward the work methods used by investigators could be reviewed.

Finally, a factor that is both an incentive and an impediment to information sharing is information technology. Described and implemented both for collecting and sharing, information technology generates handling problems. Unfamiliarity with systems, unawareness of potential, incompatibility of systems, difficulty of access, and non-access are all major obstacles that cannot be ignored. "Access to databanks is easy as long as you're able to interpret the data" (no. 17). Technology is located at the juncture between enhancing and impeding the work required to achieve the objectives.

A fourth set of factors has to do with working conditions. For some, the issue is not a matter of trying to hide information but rather of physical limitations in recording it. "There is so much information. We record some of it, we share some of it, but it's not possible to summarize a one-hour conversation....There are physical limitations to what can be recorded" (no. 13). In addition, investigators carry a heavy workload. They have to meet deadlines such as court dates. The time allotted for getting and recording the information is therefore difficult to control. "We're not really being encouraged....Once, I was told, listen, we don't have time to do the summaries, so we won't do them....There's no end to it, and I don't have time" (no. 5, 18).

So "our big problem is not the people's unwillingness, but rather the time required to supply the databanks. It's hard to convince an overworked investigator to do a summary of the collected information and to enter it into a databank that might be used the next day while he is already late for his court report on Wednesday. That's the way it goes" (no. 16).

Others feel "the big problem is the large number of databanks: everyone has his or her own little system" (no. 12). And these systems are generally not compatible with others, which causes problems with the physical sharing of hardware. "Sharing is a problem because software tools are not the same...and the transfer of information is not done" (no. 23). This also means that "the compiled data are not all the same and, as a result,...we can't help each other" (no. 20).

However, these comments come in a context where an investigator with a large police department rightly stated that informants have been computerized for several years in his department. He added, "I

have access to active sources throughout the country. It's now starting to pay off" (no. 20). A manager with the same department added later, "The amount is increasing as the culture, the understanding, the use of information, and the impacts are changing. Intelligence needs time to have an impact. I feel this will come naturally as investigators are shown what results can be achieved by sharing information" (no. 29).

Furthermore, access to databanks by members of a department is sometimes dependent on individual security levels. Restricted access is governed by administrative policies designed to protect the security of the documents. An investigator explaining the workings of a joint force operation pointed out that access to information was restricted to investigators on project X only. "We don't do it intentionally to impede the investigation. Security levels are assigned to specific individuals" (no. 8).

Finally, as previously mentioned, the storage systems and their technological tools do not always lend themselves to sharing information. Hence this important and significant comment relating to the quality and subsequent management of information: "Before we can integrate our information—because intelligence is not only info., it is a process—before we do that, we have to get our own information management together" (no. 30). In addition to considering that "the biggest problem is the large number of databanks—everyone has his or her own little system" (no. 15), investigators "don't take the time to enter their information in one system or another. If they feel their info. is useful, they will store it in a bank" (no. 15). It should also be pointed out that some police officers are still unaware of organizations like Criminal Intelligence Service Canada (CISC).

A solution proposed by a senior manager would require that databanks be made available to the individuals involved. For instance, "if NCDB is made available to all, it will take away part of the distrust which has been in policing since I was in policing" (no. 28).

In short, the following factors discourage information sharing:

1. lack of mutual trust between individuals and partners;

2. restrictions stemming from legislation and ad hoc agreements between the parties (MOU);

3. investigation work methods, including personal attitudes, methods learned on the job with colleagues, and a lack of familiarity with how computer systems work; and

4. working conditions, including investigator workloads and personnel shortages; administrative policies regarding restricted access (security levels); and a lack of familiarity with the technological tools used to manage the huge amounts of information handled by investigators.

3.3.2- Conditions for Sharing Information

Information sharing problems are offset by other factors. Various conditions for sharing information exist. These conditions reflect either an individual's personal philosophy or structural obligations. With respect to the former, some investigators feel it would be unthinkable within the framework of a joint force operation not to disclose some of the information from their department to members of other departments included in the JFO: "I am not going to hide info. from them. I do not keep secrets from them. We become ineffective, and we lose the trust at the end of the day" (no. 14). This position appears to be more a matter of personal philosophy than a formal administrative policy. The personal attitudes of investigators also fall into this category. Some stated that the involvement of various-size police departments with different databanks in a joint project gets the information moving around as required. In such cases, police officers have a direct access to these databanks. If a police officer cannot access another department's databank, an officer from that department will provide the information on request. Supplying information to the bank is also encouraged. However, after a JFO is disbanded, smaller departments are sometimes unable to access the information they provided for the investigation. Because of this, it is understandable that any interest in collecting and storing information may face major difficulties.

Also, some investigators explain their personal positions by saying, "I have some contacts. I call them, but I don't disclose my information to just anybody" (no. 20). As a concept, managing police information individually and personally seems to be applicable to all types of investigations. As stated, "The basic principle here is putting *info. belonging to you* in databanks...and you decide if you want to share it" (no. 8) (our italics). Admittedly, information ownership and the freedom to manage it create problems, but this is still an integral part of the investigation culture.

Another condition is evidence disclosure time. When this time comes, hiding the information on file is no longer an option because it will be provided anyway to the lawyers and the court. Therefore, as previously mentioned: "That's the right time to do it." Sharing information is important, but it is also important to share information at the proper time, when the evidence is disclosed to the defence (no. 9). We understand here that sharing information among investigators during the investigation is less important.

A final condition conducive to information sharing is said to be a lack of resources to efficiently conduct investigations. This condition is explained thus: "You don't keep a piece information because you know you won't be able to go all the way on account of budgetary reasons and priorities. Ultimately, you share it. What was a barrier before is less so now" (no. 17).

Conditions that provide little or no incentive for information sharing are two sides of the same problem. Both bring elements of understanding and also solutions. It nevertheless has to be acknowledged that information sharing is currently being practised, if only through the large databanks such as the Canadian Police Information Centre. This certainly is a major undertaking for law enforcement. However, for both cutting-edge and less specialized investigations, information provides not only direction but also a starting point for investigators.

In addition, information and intelligence have a different impact depending on the type of investigation being conducted. For example, joint force operations dealing with organized crime handle issues that are different from those of an economic crime unit. Still, the traditional isolation of investigation units is an

obvious stumbling block. The police knows that members of organized crime are involved in multiple activities at the same time. Their actions are divided differently than those of the police. A murder may be connected to drug trafficking or to fraud. Yet, police responses are specific and based on the description of the crime. The creation and use of joint force operations help counteract this trend. However, the collection, storage, and sharing of information remain completely taboo and restricted to the units involved. Within units, sharing information between members of different departments causes friction. Outside the units, a wall of silence and an unwillingness to share information occurs. JFOs are obviously a big improvement on the more traditional police methods used in this country. Other major reforms are needed before they are proposed as a model. One can imagine that in the not too distant future, such units will be used not only by police departments but also by bank partners, security services within large corporations, and law enforcement agencies attached to various government departments. It remains to be seen whether setting up such advanced units will impede the sharing of information between the police and their partners.

In short, the conditions for sharing information are provided below:

1. A personal philosophy based on the idea that having information makes sharing it with known individuals easier.

2. The privileged context of joint force operations against organized crime facilitates access and real information sharing, although on an informal basis.

3. Sharing information occurs at a specific time during the investigation process, particularly when the evidence is provided to the defence lawyer.

4. As the collected information could not be managed by a police department because of a lack of human and financial resources, it would be given to people capable of completing the investigation.

3.4- Databank Supply Problems

Information sharing necessarily implies that there was a prior collection period. It also suggests that the information is valuable for the investigation, the investigators involved, or the response strategies. As explained by an investigator, "We're only as good as the source we can find" (no. 9). Ultimately, information sharing is closely linked to the collection of information. However, as we will see, things are not as neat and tidy in practice.

One of the principles of data supply was accurately described by an investigator with several years of experience when he said, "An investigator needs a lot of information. If the information can't be put in a file, store it in a databank where someone else can use it" (no. 20). This shows an openness both to an active collection of information and a significant sharing potential down the line. Another item is loss of information. It seems that current investigation practices lead investigators to focus on information that is highly specific to a given investigation. The so-called secondary information is then ignored: "My notebook is crammed with information that I did not disclose because it is unlikely anyone would have been interested. I don't have time to record everything. You close your file and that's the end of it. Otherwise, we would always be busy putting info. into databanks" (no. 5). This police officer confirmed what had been previously observed by the manager of a large investigation unit: "The guys are good at collecting information but not so good at putting it into databanks" (no. 16).

Databank supply practices are affected by at least four factors. The first one deals with "how to." It is significant that an investigator pointed out the glaring shortcomings of current work methods. Discussing the collection of information, he said, "Getting information is a real burden. Each investigator has information. We have reports to do...so, we search for info. in a haphazard way. We look through databanks, etc." (no. 18). As for recording information in databanks, something significant and surprising was said. Several individuals described it in similar terms: "If I feel the information is required, I will record it, if not, I'll leave it in the file" (no. 18). The investigator does not indicate what is meant by "required." This suggests that recording information comes under investigation practices and traditional customs. Similarly, this explains the comments made by a number of investigators to the effect that less

than one-eighth of all potentially relevant information is stored in databanks. "What is irrelevant to one investigator might not be to another" (no. 17). Here again the workload carried by investigators becomes an argument for a partial or non-supply of databanks. "We must avoid supplying several databanks at the same time. Given their current workload, it is unrealistic to assume that investigators will be able to write their reports and also record their information in databanks" (no. 16). Another comment: "Recording everything is a big job. You have personal notes, a report to write, the event report. It never stops. You have to do the summary. I don't have time" (no. 22, 18).

The second factor involves information sources. What should be collected. Most investigators interviewed agreed that the collected information must be current and up to date so that it can be used for investigations. The process of collecting information and checking its relevance is considered demanding (nos. 5, 9). The idea is that once the information is collected, its validity has to be checked, to make sure it is not just gossip, but usable information for an investigation (no. 20). When information collection is described this way, it is not an inducement to supply databanks because of this idea that non-validated information is just gossip. Yet, as mentioned earlier, what is irrelevant to one investigator might not be to another. Intelligence is seen by several investigators as directly relevant to the investigation, to the extent that it could be submitted as evidence in court or used to make arrests or get convictions. "Intelligence is usable as evidence to make arrests and get convictions....It can also be used for operations" (no. 7).

The third factor involves information sources. Once again it is a matter of checking whether there is a methodological process in place to get the most benefit from potential sources. As expected, the main source is said to be in the field, which implies getting out of the office, making contact with individuals, and doing active surveillance (no. 13). During the collection process, investigators need to develop a habit of considering the overall event, thus allowing for the possibility that a minor detail could become a key to solving the crime. Another active source is the patrol officer. He or she provides information for specific cases (no. 16). In the "person under surveillance" (PSU) concept created by the *Sûreté du Québec*, patrol officers know immediately what to do, and they act accordingly when intercepting suspects. They state the reason for intercepting the individual and indicate if they require additional

information (no. 21). The patrol officer acts as a transmission medium: although investigators may sometimes give the officer information, they more often contact him or her to get information.

Finally, the fourth factor concerns the impact of technology. This impact is said to be measured based on use. Nevertheless, it appears that people do not have access to the technical resources they need. "We do not have the technical resources to technically service our NCDB. We are not putting enough info. into the system (no. 14). Another explanation is a lack of human resources to transfer the info. into databanks. Some feel that although a lot of information is being collected, not enough people are available to enter it (no. 11). A similar comment was made: "We found that those departments that do supply the databanks have people dedicated full time to this task" (no. 16).

In short, databank supply practices are affected by four factors. They are:

1. "how to," which refers to the work methodology or lack thereof;

2. what should be compiled, which emphasizes that supply practices are encouraged within the framework of specific and less specific investigations to provide a basis for the creation of criminal intelligence databanks;

3. direct information sources known both through traditional techniques and the contribution of patrol officers; and

4. information collection supported by technology, provided this technology is used and is designed to help investigators.

4- The Need for Adequate Training

The need for adequate training was clearly recognized by the people interviewed and by many others involved in law enforcement. There is no question that adequate and adapted training helps achieve quality work. Some will say this training must be specialized so that police officers can remain current in their area of expertise. Training becomes in fact one of the crime-fighting tools in the sense that "every component is vital to the end result" (no. 3). For this to occur, training must be provided in a timely fashion, which does not seem to be the case for a large majority of those interviewed, either because there is too much staff rotation or because new investigators are picked directly from the patrol ranks and there is not enough time to train them adequately. Finally, one of the main problems with investigator training, although not exclusively related to training, is personnel rotation. Even if a manager drafts an annual training plan for members of his or her unit, individuals still have to change units because of the promotion process. This means that sometimes incumbents are not trained, or, if they are trained, they may have to move to another unit. As stated: "The biggest problem is police officer rotation. You're with a unit, you get trained and you move to another unit. The organization is left in a position where all it does is train individuals who, although highly dedicated, have no experience....All this training is a waste because people move all the time" (no. 17).

Officers sometimes learn their job in the field over time. It is said that "it takes time to learn" (no. 6). This situation is not the target of criticism or negative comments. The individuals who were interviewed were hoping that investigators would eventually hone their skills on the job. "With a less-experienced workforce, young officers come in directly from their patrol cars. They learn on the job. They eventually become proficient" (no. 12). Stated in a different way, learning is "getting advice from others; you learn by asking others" (no. 6). Also: "I learned by asking anyone around me. I got information anywhere I could" (no. 22).

Still, some were able to assess the impact of a lack of adequate training or the use of partial training, on the job, with colleagues not always more experienced than they are. For example, an investigator with a large department observed that 75% of all new investigators come directly from patrols. They have no

investigative experience, no skills, no interest; they're lost (nos. 3, 4, 9), and their initial training is hardly relevant. This has two immediate consequences. First, individuals with little or no training have to rely on others for information and advice. This means a significant waste of time for both the newcomers and the experienced officers. These individuals have to create their own support network to get relevant information or they have to find adequate contacts. "If we can't get the information, we contact someone well informed....This is a waste of time both for him and for us" (no 18). Also: "If I'm not in a position to investigate...I will get in touch with a contact to get some leads....I will ask for references or specific information" (no. 22). Furthermore, the need to constantly rely, at least for a time, on someone else could potentially lead to mistakes or make people reluctant to act. "He is left to himself, he manages on his own. It's not easy. Sometimes he goes too far in one direction or another. He runs around in circles because he doesn't know where he's going....I've often seen people misinterpret information and tell falsehoods." Even more dramatic consequences can ensue, where expensive cases are lost because of legal errors. "When police officers are making mistakes, it is a huge backward case law....We are losing taxpayers' money..." (no. 2).

We asked individuals if specific topics or issues should be included in training programs. One felt that what was needed was not necessarily the development of training programs, but rather a greater emphasis on cutting-edge and customized training. In this way, the specific needs of typical clients could be met, especially in the area of information technology. "The problem with technology is its rapid advance. I don't know of any training school that can keep up....We've been focusing on customized training. We want our people to return to a standard base" (no. 19). Some also stressed the importance of encouraging individuals to remain up to date with developments in their area of expertise. Called "indirect training," it helps individuals "remain alert, well informed on their environment, aware of trends...etc." (no. 19).

Training includes also and especially the development of legislation and case law. Both have an impact on work practices and methods. As a manager observed, "You have to keep up to date" (nos. 9, 2). In addition, training covers law enforcement skills and techniques, practices with informants, adequate use of databanks, infiltration of organized groups, languages used, etc. (nos. 4, 9, 2, 3).

Investigator training, especially on organized crime and cybercrime, was not systematically provided to interviewed officers no matter what their police department was. More often than not, training is done on the job using contacts and requests between colleagues, with the more experienced providing guidance to the newcomers. The beginner and advanced investigator training programs are seen as relevant by those who took them—very few of the people interviewed. On the other hand, there is a consensus on the need to keep investigators up to date with legislation, case law, and developed skills because they are said to directly affect investigator practices and results. With respect to technology, some feel that customized training is better able to meet the needs of officers.

Some of the people interviewed pointed out that specific budgets are too often affected by cuts. Although effective in the short term for police managers, these cuts definitely affect police practices in the long run by producing police blunders, legal errors, or simply improper investigative methods.

In an ideal world all reported crimes would be investigated. Some would be solved by investigation and intelligence professionals. Yet, in the real world, citizen complaints are often disregarded because of a lack of time, financial resources, or simply understanding of the complexities of the complaint. If accepted, some complaints are subsequently investigated, sometimes thoroughly, sometimes not. It could be said that the results depend to a large extent on the skills and professionalism of the police officers who receive and investigate the case. In a rapidly changing environment, it is all the more critical that the training given to investigators be compatible with this environment.

In short, it appears that training on investigations and cybercrime investigations is inadequate. Those interviewed seemed to feel that the training provided was insufficient.

Similarly, it appears that the training programs are not sufficiently compatible with the new reality faced by investigators. The police cannot keep up with society.

Also, training program updates cannot keep pace with the technology market. Although it is true that an investigator must first learn how to investigate before learning how to investigate cybercrimes, the fact

remains that adjustments are required to deal with technological advances that make completely new and revolutionary responses possible.

4.1- Development of Critical Success Conditions

The statements made by some of those interviewed suggest that criminal investigations, especially cybercrime and organized crime investigations, have complex and interesting dynamics. We observed that discrepancies often existed between what people claim they do and what they actually do in their daily practices, based on their skills, prior training, personal interests, and available budgets. We also looked at initiatives involving several police departments, if not the collection and sharing of criminal information and intelligence. We commented elsewhere on what items should be included in a training program for investigators, particularly for emerging crimes. One last point should be discussed. It has to do with police success factors in fighting crime. Although it is true there is a large body of literature on continuous and recruit training programs, there are not as many publications on how training programs meet their objectives. We are not referring to the objectives of a course but to broader objectives concerning the use of any given content and, above all, about the relationship that exists between individuals and this content. In other words, if individuals have no confidence in what they are taught or are unable to apply what they have been given, practices cannot be improved.

Conditions for an investigation to run smoothly include a large enough staff, an adequate budget, relevant training, use of cutting-edge technology, etc. Training programs have no impact on most of these factors. However, they may potentially affect attitudes and feelings. They can also enhance individual skills. However, to achieve this, a number of bridges still have to be crossed.

In his book on computer crime investigation techniques, Mendell (1998) looks at the overall information technology environment. He makes a very convincing statement on the future success of training and investigation when he explains that "intelligence seeks to perceive what is not immediately apparent. By integrating both rational facts and intuitive insights, intelligence offers a holistic picture" (p. 53). The real challenge for investigators, and we should also include analysts here, is to sort out the facts using their

judgment, intuition, and deductive powers. These aspects are all the more important because information technology has created new means of communication, a new language, new ways of doing business, and its own phenomena called hacking, cracking and phreaking. We're already using the phrase hacker culture (Taylor, 1999) and many others. It also seems that a generation gap has opened up among hackers, as the younger ones have grown up with a computer at home. Police officer training programs probably do not emphasize enough the qualities to be developed because to do so would require a major personnel investment over the short and long term and would involve a certain departure from the classroom-as-a-magic-solution principle. These qualities seem to be directly linked to the information technology culture. This requires not only understanding the language of computers, but also becoming familiar with the new environment created by computers.

In a fast-changing world, future investigators will need to have the following qualities: experience, proficiency, good analytical abilities, and enough flexibility to adapt their work environment to technological advances, future legislation, and the enforcement of this legislation. Another benefit would be the creation of a network system with the help of high-tech companies. (See, among others, Meyer, Short, 1998.)

Like Mendell, we feel investigator training should not only cover techniques, which it already does, but also include exercises in logic, deduction, and assessment of difficult cases. Scenario-type exercises should encourage student input while testing students' understanding, development capacity, and their deductive abilities. As Boni and Kovacich rightly pointed out (1999:36), one of the biggest challenges faced by law enforcement and modern security is learning to think and operate in a new dynamic environment created by technology.

Other potential solutions should be explored. They include partnerships between the police and various groups involved in security. They also involve alliances with government agencies and other countries. The ultimate goal is to prevent crime, including organized crime and cybercrime. Keeping these partnerships up to date is the real challenge. Each organization has to follow legal standards, work practices, and ethical rules. Furthermore, because of pressures exerted by elected officials to get law

enforcement agencies to review their approaches to the community, to give a higher priority to crime victims, and to control their operating costs, victimless crimes are given less attention. Yet, investigating this type of crime is very demanding in terms of human and budgetary resources (shadowing, operational support, wiretapping, physical surveillance). As stated, "major losses suffered by corporations, which are perceived by local officials as victimless crimes, are a reality. Presently, there is a danger municipal authorities will say, "We'll take your case but our only resources are our investigators. We'll need money to pay informants and to pay for our support to the operation....This is done quite often now" (no. 31).

What is at stake? What is the information sharing capability of each? What tools are available to do this? What limitations are placed on sharing personal information by privacy legislation? What are the technical hurdles? These are major issues that need to be addressed to be able to achieve partnerships to fight crime. There is also the fact that private industry is willing to co-operate with public security only up to a point. They are generally unwilling to put at risk their privileged relationship with their customers, i.e., the members of the community.

Presumably, tools, work methods, and common interests could be shared through seminars providing advanced training consistent with the reality of the organizations involved. These could probably be structured on the basis of on-line or distance training (Mulholland, 2000).

Partnerships can also be demonstrated through specific co-ordination among law enforcement agencies. One can envision the development of a databank that would be used, for example, for sophisticated technological crime or for action models to be able to develop prevention programs. One can also foresee the development of a list of law enforcement players or units dedicated to organized crime and cybercrime. Surveys conducted by specialized firms on the penetration of computer systems could be very helpful to the police for their decision-making process.

One pragmatic approach is worth mentioning. The US Justice Department (2000) developed a Web page for children where information is provided on what the Internet can do and what it should not be

used for. A similar Web page was developed to educate the general public on how to deal with the changing Internet environment. The rationale is simple. As technology provides direct and immediate access to all sorts of information from a wide range of sources, individuals need to develop an Internet use ethic, an ethic that should obviously be developed as early as possible when growing up. Another recent initiative was the creation of a computer science laboratory in the San Diego area through a partnership between federal, state, and local law enforcement agencies. By putting their resources together, they significantly increase their potential (Robinson, 2000).

Conclusion

This report discusses information collection, databank supply, and information sharing between police officers and police departments. It focuses in particular on organized crime and cybercrime, two complex and emerging areas of investigation.

We looked at how police officers, crime analysts, and decision makers perceive investigation procedures and what solutions they have in mind. This last aspect is not very substantial.

We felt that once the hurdles and current success factors had been identified, it would be possible to foster information sharing, improve individual performance, and maybe create national standards for information collection, security levels, and approaches needed to develop trust between partners.

Existing limitations affecting investigations can be summarized as follows: There is a staff shortage, and the personnel is constantly being rotated. For instance, investigators from the homicide unit are sometimes seconded to other units. The computer crime sections may also be too small. Also, individuals frequently have to leave an investigation unit to be eligible for a promotion. These investigators take their expertise with them, and they have to develop another.

In addition, several people interviewed argued that budgets are often inadequate or insufficient to provide the tools required to conduct effective investigations.

Investigator training is not always suited to the context, is not always timely, or is not received at all. Yet, it is essential. A training program obviously has to cover legislation and case law. In addition, these topics remain one of the pillars of investigations. It is therefore critical to have a detailed knowledge of Part VI of the *Criminal Code* concerning affidavits. Other training aspects relate to skills that must be developed to work with colleagues within one's own department or in other departments or law enforcement agencies.

For information technology-related crimes, there is a requirement to develop investigative skills aimed at understanding what to do rather than trying to become an expert in data processing or systems management. There is a large pool of experts in the field of technology; police officers simply have to learn to work with them.

Several types of databanks are used within the public security community. Some are at the national level, such as the Canadian Police Information Centre, while others belong to specific organizations, such as the RCMP's NCDB, or government departments, such as Customs and Excise, etc. Also, access to these banks is complicated. Various levels of security are used for members of a police department and for other police departments. Furthermore, the incompatibility of computer systems is a major problem. Added to this is the databank supply issue, which involves the extent to which individuals trust these banks and the time available to enter the information. Finally, data quality is an information issue that is generally overlooked. Although information should help make sound decisions during an investigation, not enough emphasis is placed on the relevance of this information. Once police officers have crossed the need-to-know and right-to-know thresholds, hurdles remain with respect to openness between colleagues, mutual trust, and the physical capability of sharing information.

It can be safely said that, to date, there has been an obvious lack of awareness of problems and issues concerning cybercrime, computer terrorism, and new types of environmental crimes. More often than

not, those interviewed thought these came under the responsibility of specialized units or agencies other than the police. This suggests that law enforcement does a poor job of preparing the officers to deal with an evolving society.

Finally, one last comment. There definitely is an investigation culture. In this culture, individuals are kept in boxes, sometimes referred to as silos, which is an impediment to co-operation among colleagues, to information sharing and, finally, to a successful investigation. A potential solution would be to use joint training programs where co-operation, sharing, and the ability to get expertise wherever it can be found would be taught and encouraged. Today, sharing is still done unilaterally from the police to various agencies, from large departments to small ones, and with large companies that are willing to co-operate with the police. This is counterproductive in the medium and long term. We therefore need to develop a less restrictive intelligence culture.

One proposed approach would focus on the types of partnerships to be achieved with other law enforcement agencies, based on best practices and major lessons learned. This approach would also emphasize potential partnerships with private police services and security agencies used by large corporations such as banks. The approach would further concentrate on opportunities for partnerships with large industries in the area of information technology. These industries are responsible for developing tools for society. It is up to the police to design approaches that are compatible with these tools.

References

Alexander, K.; Munro, R. (1996). Cyberpayments: Internet and Electronic Money Laundering: Countdown to the Year 2000. *Journal of Financial Crime*, 4, 2:156-160.

Benson, D. (1993). The Police and Information Technology. In G. Button (ed.) *Technology in Working Order*. London: Routledge.

Blackburn, W. (2000). Credit Card and Debit Card Fraud in the Year 2000. *The Report on Crime & Profiteering*, 4,1:6.

Boni, W; Kovacich, G. (1999). *I-Way Robbery. Crime on the Internet*. Boston: Butterworth Heinemann.

Canada, Department of Justice. (2000). Electronic Commerce. Http://Canada.justice.gc.ca. Consulted 00/09/15.

Canada, Federal Government (1998). Joint Statement on Organized Crime. Federal-Provincial-Territorial Ministers Responsible For Justice. Regina, Canada, October 30, 1998.

Carter, D.; Katz, A. (1998). Computer Applications by International Organized Crime Groups. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

CSIS Global Organized Crime Project (1998). *Cybercrime, Cyberterrorism, Cyberwarfare. Averting an Electronic Waterloo.* Washington: CSIS.

Davis, R.; Hutchison, S. (1997). *Computer Crime in Canada*. Toronto: Carswell.

Deloitte Touche Tohmatsu (1999). Cracking Computer Fraud: A U.S. View. *The Report on Crime & Profiteering*, 3, 1:6-7.

Denning, P.J. (1998). The Internet after Thirty Years. In Denning D.; Denning, P. (ed.). *Internet Besieged. Countering Cyberspace Scofflaws*. New York: ACM Press.

Dertouzos, J.; Larson, E. ; Ebener, P. (1999). *The Economic Costs and Implications of High-Technology Hardware Theft*. USA. CA, Santa Monica: Rand. Science and Technology Program.

Drolet, J.F.; I. Moen (2000). Enabling the Next Generation of Defence Capability. Nanotechnology. *Vanguard*, 6:22.

Dryden, J. (1998). La montée en puissance du commerce électronique. L'Observateur, nº 214, octobre-novembre, www.oecd.org//publications/observer. Consulted 1999/02/10.

Ekos Research Associates Inc. (2000). The Public Opinion Environment and Emerging Trends in Public Security. Presentation to SEC/Co /Directors Planning POWPM. March 28.

Federal Bureau of Investigation (1999). Encryption: Impact on Law Enforcement. www.fbi.gov/library/encrypt/encryppt.htm. Consulted 00/04/12.

Field, M. (2000). Organizational Dynamics in a Technology-Driven World; The Impact of Email on Law Enforcement, *The Police Chief*, February, 45-49.

Hamilton, H. (2000). The Effective Use of Partnerships to Reduce the Impact of Organized Crime: How Ontario' CFSEU Balances the Responsibility. *The Gazette*, 62,3: 17-23.

IACP (1999). Best Practices for Seizing Electronic Evidence, www.theiacp.org. Consulted 00/04/12.

Icove, D.; Seger, K.; VonStorch, W. (1995). *Computer Crime. A Crimefighter's Handbook*. Sebastopopl, CA: O'Reilly & Associates, Inc.

LeBeuf, Marcel-Eugène (2000a). *Policing and Use of Information Technology: An Assessment*. Ottawa: Police Sciences School, Canadian Police Collège. Available at www.cpc.gc.ca.

LeBeuf, M.E. (Ed.) (2000b). Police and Information Technology: Understanding, Sharing and Succeeding, May 28-30, 2000. *Conference Proceedings*, September. Ottawa: Canadian Police College (CD-ROM.).

LeBeuf, M.E. (2000c). *The Implications of Using Information Technology for Police Investigators in Canada*. Ottawa: Police Sciences School, Canadian Police Collège. Available at www.cpc.gc.ca

LeBeuf, Marcel-Eugène, Paré, Simon; Belzile Miguel (1999). *Canadian Police Information Technologies: Current Overview*. Ottawa: Police Sciences School, Canadian Police Collège. Available at www.cpc.gc.ca.

Lenton, W. (2000). Official Welcome. Pacific Rim Money Laundering & Financial Crimes Conference, Vancouver, October 20-24.

Livanos Cattaui, M. (1999). Alliance Against Commercial Cybercrime. Conference Report. International Chamber of Commerce. London, 7 December. Http://www.iccwbo.org/home/conferences/reports. Consulted 00/20/10.

Mendell, R. (1998). *Investigating Computer Crime. A primer for Security Managers*. Springfield: Charles C. Thomas Publisher Ltd.

Meyer, J.; C. Short (1998). Investigating Computer Crime. Police Chief, www.theiacp.org Consulted 00/12/04.

Mulholland, David (2000). Technology Training and Education Opportunities, Police Chief, 03/03/2000, www.theiacp.org. Consulted 00/04/12.

Murray, A.D.; Vick, D.W.; Wortley, S. (1999). Regulating E-commerce: Formal Transactions in the Digital Age. *International Review of Law Computers & Technology*, 13,2:127-145.

Nations Unies, Rapport du Secrétaire général (1999). Situation de la criminalité et de la justice pénale dans le monde. *Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants*. Vienne, 10-17 avril 2000.

Norman, D. (2000). The State of On Line Learning. *Training*, September.

Organized Crime Digest (2000a). Teens Arrested for Cyber Fraud. (January) 21,2:3.

Organized Crime Digest (2000b). Internet Thefts Create New Risks. (March) 21,5:5.

Organized Crime Digest (2000c). 29 Nations Will Work for Uniform Policies Against Cyberfraud. (August), 21,16:3.

Osterburg, J. W.; Ward, R. (1997). *Criminal Investigation: A Method for Reconstructing the Past*. 2nd ed. Cincinnati: Anderson Publishing Company.

Parsons, M. (1998). Crime Prevention and the Electronic Frontier, FBI Law Enforcement Bulletin, www.fbi.org. Consulted 00/04/12.

Porteous, S. (2000). The Greening of Intelligence. *Crime & Profiteering*, 4, 3:13-14.

Porteous, S. (1998). *Organized Crime Impact Study. Highlights.* Ottawa: Public Works and Government Services Canada

Richards, J. (1999). *Transnational Criminal Organizations, Cybercrime, & Money Laundering: Handbook for Law Enforcement Officers, Auditors, and Financial Investigators*. Boca Raton: CRC Press.

Robertson, J. (1999). The Changing Face of White-Collar Crime, *Police Chief*, www.theiacp.org. Consulted 00/04/12.

Robinson, M. (2000). Law Enforcement Response to Cyber-Crime. Police Chief, www.theiacp.org. Consulted 00/04/12.

Royal Canadian Mounted Police (2000). Environmental Scan 2000. Trends. www.infoweb.a.rcmp-grc.gc.ca.

Sambugaro, E. (2000). Cyberspace and the Criminal E-economy. *The Report on Crime & Profiteering*, 3,4:4-5.

Sambugaro, E. (1999). Cybercash Aids Organized Crime Money Launderers. *The Report on Crime & Profiteering*, 3,3:7.

Scientific American (2000). Internet Anonymity. Speech without Accountability. October:34.

Sheriff (1999). Computer and Internet Crimes, www.theiacp.org. Consulted 00/04/12.

Smith, R. (1999). Defrauding Governments in the Twenty-first Century. *Trends & Issues in Crime and Criminal Justice*, no.111. Australian Institute of Criminology.

Soullière, Nicole (1999). *Police and Technology: Historical Review and Current Status.* Ottawa: Police Sciences School, Canadian Police Collège. Available at www.cpc.gc.ca.

Sullivan, S. (1999). Policing the Internet, FBI Law Enforcement Bulletin, www.fbi.gov. Consulted 00/04/12.

Taylor, P. (1999). *Hackers. Crime in the digital sublime*. London: Routledge.

TELEMASP Bulletin (2000). An overview of computer-related crime. *TELEMASP Bulletin*,7,1:1-11.

The Report on Crime & Profiteering (2000). "GetRichQuick.com": FTC Sweeps the Internet for Scammers. 4,1:9.

Thompson, E.P. (1975). *Whigs and Hunters. The Origin of the Black Act*. New York: Pantheon Books.

U.S.A. Department of Justice (2000). Cyber Ethics, www.cybercrime.gov. Consulted 00/10/20.

U.S.A. Government (1999). Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice-President. www.theiacp.org. Consulted 00/04/12.

Wall, D.S. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law Computers & Technology*, 12, 2:201-218.

White, L. (2000). Ernst & Young Survey Finds a New Generation of Fraudsters. *The Report on Crime & Profiteering, 4,2:7.*

White, C. (2000). Egg Bank Robbery: Cyber-bandits on a Roll? *The Report on Crime & Profiteering*, 4,3:17.

Williams, W. (1999). The National Cybercrime Training Partnership. *The Police Chief*, February: 17-27.